Mobile and Forensics
Vol. 6, No. 2, September 2024, pp. 25-33
ISSN: 2714-6685 (online), 2656-6257 (print)
DOI: http://dx.doi.org/10.12928/mf.v6i2.11287

National Institute of Standard Technology Approach for Steganography Detection on WhatsApp Audio Files

[1,*]Abdul Haris Muhammad, [2]Gamaria Mandar
[1,2]Department of Informatics,, Faculty of Engineering, Universitas Muhammadiyah Maluku Utara
[1,*]agry.arisandi@gmail.com, [2]gamariamandar20@gmail.com
[*]correspondence email

Abstract

Audio steganography in instant messaging applications such as WhatsApp poses new challenges in the field of digital security, especially due to the ability to hide data in frequently used formats. This research examines the effectiveness of steganography detection on WhatsApp audio files by applying a method developed by the National Institute of Standards and Technology (NIST). This approach was chosen due to its reputation in security testing standards, but its use in the context of audio steganography on instant messaging platforms has not been widely explored. The novelty of this research lies in the adaptation of the NIST method specifically for audio steganography analysis in WhatsApp, which includes testing against various compression and end-to-end encryption scenarios. The main findings of this research show that the NIST method successfully improves the accuracy of hidden message detection compared to conventional steganalysis techniques, especially under the condition of compressed audio files. In addition, this research also found that the integration of the NIST method enables more effective detection of steganographic data in encrypted audio files. These results confirm that the NIST method can be successfully adapted for instant messaging applications such as WhatsApp, making a significant contribution in the improvement of digital security. This research not only identifies weaknesses in existing steganography techniques, but also introduces a new framework for more accurate and efficient detection in encrypted environments.

Keywords: Audio File, WhatsApp, Steganography, NITS, Mobile Forensics

INTRODUCTION

WhatsApp instant messaging application is one of the most widely used applications because WhatsApp messenger is not only a medium for sending messages in the form of text only, but also can send messages in the form of video and audio or sound[1][2][3]. In addition, WhatsApp Messenger also has a high level of security, namely with end-to-end encryption, where messages sent are encrypted to avoid criminal acts[4]The very significant use of WhatsApp is because its users make WhatsApp as one of the platforms to convey messages without being limited by time and space[5]. However, this application also has a negative side to commit cybercrime[6]. One of them is the use of audio steganography in instant messaging applications such as WhatsApp provides new challenges in the field of digital security[7], especially because of its ability to hide data in frequently used formats[8][9]. In addition, some of the challenges faced when analyzing audio files on WhatsApp are, data compression, namely this application performs data compression techniques when a file is sent, of course, it can change the pattern of data inserted through steganography, making it difficult to detect a message[10][11]. Then end to end encryption, where the WhatsApp application uses end-to-end encryption for all messages sent, including audio files[12][13]. This encryption protects the content from third-party access, but also makes steganographic analysis more complicated because the data must be decrypted before it can be analyzed[14], which usually cannot be done without access to the encryption key and various types

Article History: *Received August 5, 2024; Revised August 24, 2024; Accepted August 26, 2024*

of audio formats such as MP3, AAC, WAV, and OPUS[15]. Each format has different structures and characteristics, so the steganography techniques used can vary and require detection methods that are specific to each format[16][17].

This approach was chosen due to its reputation in security testing standards, but its use in the context of audio steganography on instant messaging platforms has not been widely explored[18][19]. The novelty of this research lies in the adaptation of the NIST method specifically for the analysis of audio steganography on WhatsApp, which includes testing against various compression scenarios and end-to-end encryption[20]. The main findings of this study show that the NIST method successfully improves the accuracy of hidden message detection compared to conventional steganalysis techniques, especially under the condition of compressed audio files.

In addition, this study also found that the integration of the NIST method enables more effective detection of steganographic data on encrypted audio files. These results confirm that the NIST method can be well adapted to instant messaging applications such as WhatsApp, making a significant contribution in the improvement of digital security. This research not only identifies weaknesses in existing steganography techniques, but also introduces a new framework for more accurate and efficient detection in encrypted environments.

METHODS

In this study, the investigation process refers to two methods: the National Institute of Standard Technology (NIST) method, which has several basic stages in the forensic process: collection, examination, analysis, and reporting. This method is used to carry out the acquisition process on a smartphone with a WhatsApp application, while the audio steganography analysis process uses the Spread Spectrum method.

Proposed Method

At this stage, smartphone acquisition aims to get audio files stored on the WhatsApp application using the following steps in the NIST method:

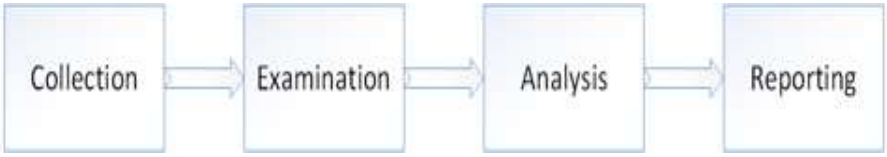

Fig. 1. The National Institute Standart of Technology Method[3]

Collection: at this stage, data collection is carried out on the whastapp application to find evidence in the form of audio files sent to the victim. Examination: In the next step, there will be a process of identifying data that can be used as evidence. Once determined, the data will be retrieved, the data retrieval process will be forensically tested. Analysis: The data that has been taken will be analyzed to look for things that can be used as evidence, especially data on the application. evidence, especially data on the WhatsApp application. Reporting: The final stage of the forensic step to find audio files on the WhatsApp application is reporting the results of forensic analysis from start to finish in the form of a written report so that it can provide recommendations for improving policies, guidelines, procedures, tools, and other aspects of the forensic process.

Audio Steganography Method

In this research, the audio files used the audio steganography technique using audio steganography method.

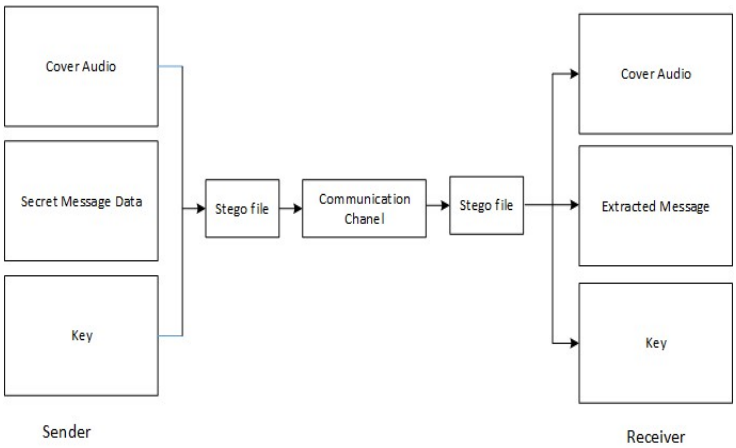

Fig 2. Audio Steganography Method[15]

In this research, a method approach is proposed by implementing a multi-encryption process where the first encryption pattern uses a matching algorithm to encrypt a message into an audio file, then utilizes the least significant bit (LSB)[21]. After the message is inserted into the audio cover, the result is a file called a stego file. This stego file is then sent through the WhatsApp application to ensure the security of the message remains safe, during transmission, the stego file looks like a normal audio file, so it does not arouse suspicion. The LSB technique uses a key to increase security by randomizing the position where the message is inserted, so that only recipients who have the key can extract the message. This method is divided into three parts, namely the compression process in which the audio file to be encrypted is first subjected to a compression process with the aim of avoiding detection[22], then the second stage is the encryption process The encryption process converts the audio file to be sent to binary data, while the receiver undergoes a decryption process to reveal the contents of the encrypted file, and the third process is the embedding/deembedding process This process deals with hiding the secret file into the secret file into the object while the receiver at the destination undergoes the de-embedding process by extracting the file[23].

Case Scenario

The purpose of this case scenario is created and run in order to facilitate the investigation process. This research creates a case scenario that is run on WhatsApp on an Android smartphone, which can be explained in Figure 3 with the following scenario flow:
First, the suspect (Account A) initially sends a threatening message to the victim (Account B) after sending several messages in the form of text, the suspect then sends a file in the form of audio to the victim (Account B), then the victim (Account B) tries to open the file, but the file when run or played sounds a voice but is unclear and cannot be understood by the victim (Account B), then the victim (Account B) reports to the authorities or police to reveal the contents of the message contained in the audio file.
The authorities then issued a warrant to search the suspect (account A) to secure electronic evidence, namely a Xiaomi Redmi Note 10 Pro smartphone used to make threats and send audio files via the WhatsApp application.

Figure 3. Case Scenario

One of the stages that a digital forensic investigator must carry out is The Chain of custody to secure and protect digital evidence. In this study, digital evidence is messages and audio files on the WhatsApp application. All data on WhatsApp related to the case scenario above will be analyzed on the victim's device (account B).

This research, of course, requires supporting tools to perform forensic analysis. The tool is divided into two, namely hardware and software. The hardware used is a Lenovo laptop and Xiaomi Redmi Note 10 Pro Smartphone, while the software used is Mayestik rooting and Final Mobile Forensic.

Smartphone Acquisition

The first step is to confiscate one Redmi Note 10 smartphone belonging to the victim (account B), then carry out acquisition and analysis to find data and information contained in digital evidence. Then, the tools and materials used to collect all potential digital evidence are complete

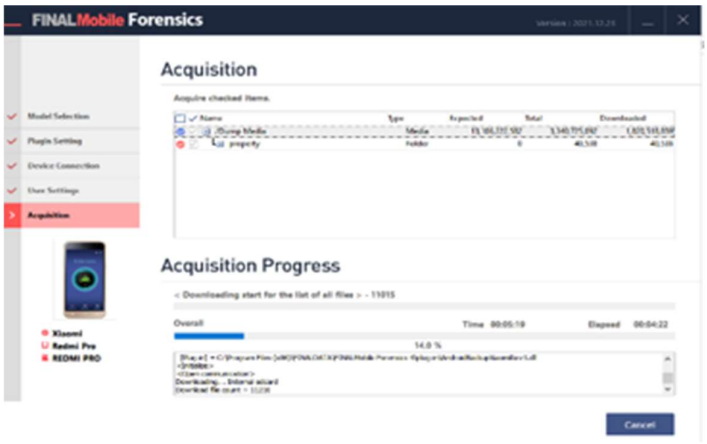

Figure 4. Evidence Acquisition Process on Smartphones

Based on figure 4 shows the process of acquiring Xiaomi Redmi Note 10 Pro smartphone evidence. There are items that are the goal or target of acquisition, namely dump media and property. In dump media, the total file downloads are 1,820,518,859, while in property, there are a total of 40,539 downloads.

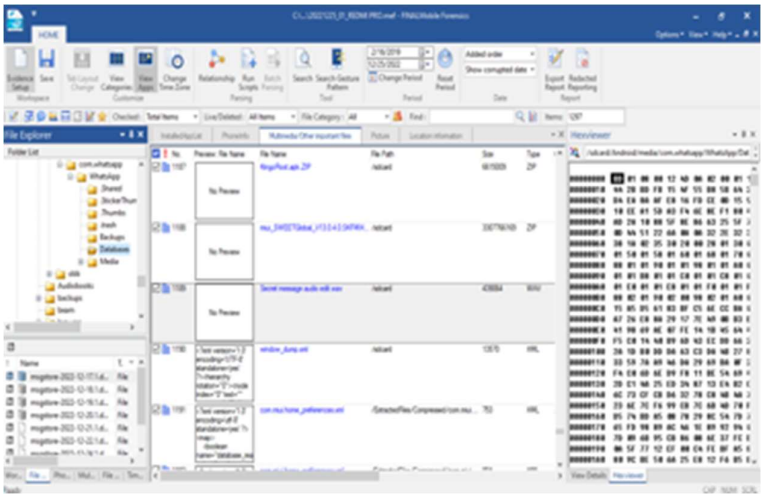

Figure 5. Analysis of Smartphone Evidence

Based on Figure 5, it can be explained that the process of analyzing evidence in audio files is found at the filelocation/sdcard/Android/media/com .WhatsApp/WhatsApp/Databas e/ with the name Secret message audio edit.wav with data type Multimedia/Other Important files, which means that the file is sent via WhatsApp which is then stored in the database with a file size of 428.8 KB and last write time 2022-12-20 AM 09:11:49 and then export the file to be analyzed at the next stage.

Audio File Analysis

After acquiring the smartphone evidence, an audio file was found, which was then analyzed to obtain information. This analysis uses Audacity audio tools to perform spectrogram and frequency analysis to determine the frequency distribution in the audio file.

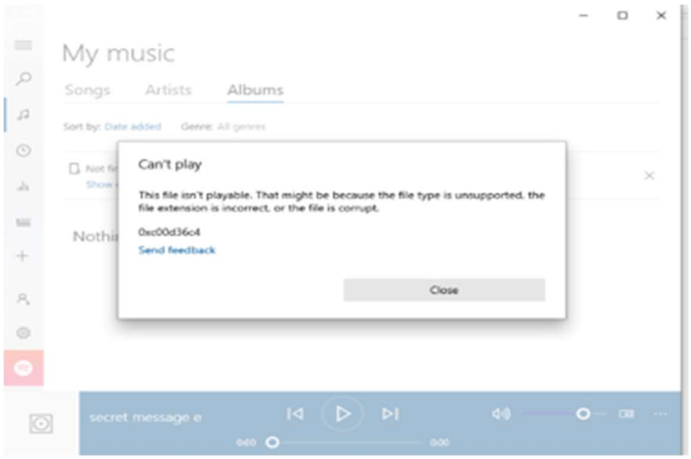

Figure 6. Error Secret Message Audio File Edit.wav

Based on figure 6, when the audio file is run, there is a statement that the file is an error or corrupt with the code 0xc00d36c4. The corrupt file is then suspected of being an encrypted file, so it needs to be decrypted in order to find the information in it. The decryption process is carried out

using several scripts, which are then run to get the key file. In the file, there is a key with the valu e b'87Iq5Dz3sDPHD2Ez0f6DMLcBElvuESVfaClLNMAdneQ=', which is then used to decrypt.

```
In [12]: fernet=Fernet(key)

with open('secret message edit.wav','rb') as enc_file:
    encryoted=enc_file.read()

decrypted=fernet.decrypt(encrypted)

with open('secret message edit dec.wav','wb') as dec_file:
   dec_file.write(decrypted)
```

Figure 7. Decryption process of Audio Secret Edit.wav file

Based on figure 7, After decryption, the frequency of the sound is analyzed using the spectrogram method to see the information from the file sent by the perpetrator (account A) to the victim (account B).

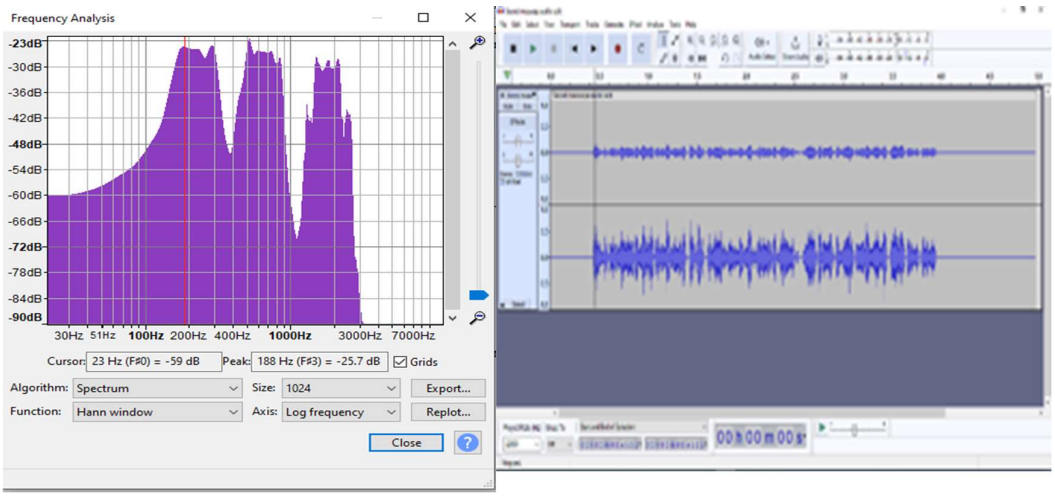

Figure 8 Frequency analysis of the Secret Edit.wav audio file

Based on the figure 8, it can be explained that there are several changes in the spectrogram in the audio file being analyzed, namely changes that occur suddenly can indicate data or message insertion. Analysis of Frequency Changes The initial frequency is at 30 Hz which is in a very low range, then there is a very significant increase of 100 Hz. This increase can indicate the beginning of the data insertion process or audio manipulation, then an increase occurs from 100 Hz to 1000 Hz, this increase is suspected of data or information being hidden which usually does not occur in audio files consistently. This significant change in frequency can indicate the insertion of a message or data through steganography techniques. These changes are designed to be undetectable especially if they only occur for a short period of time at different frequency ranges. Then the change in frequency variation from 30 Hz to 1000 Hz over a wide enough spectral range can be used to hide more messages especially if frequency-based steganography techniques are used, whereas unusually large frequency spikes over a short period of time are a common characteristic of intentional signal manipulation to hide information.

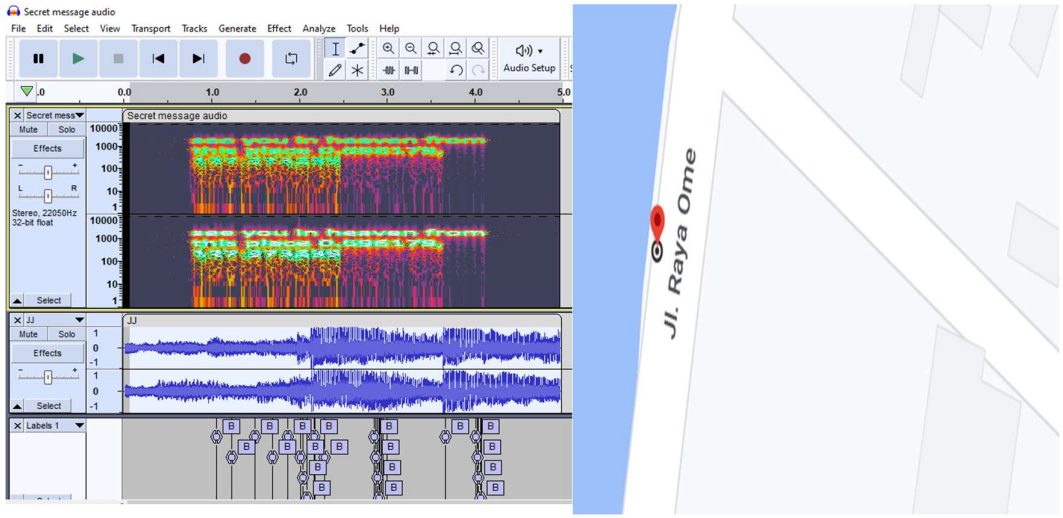

Figure 9. Spectrogram analysis of secret message edit.wav audio file

After analyzing the frequency and then analyzing the spectrum of the audio file, a text message with a JPG extension was found, and it read, “See you in heaven from this place.” Then, there are the numbers 9.696179 and 127.373239. From the above spectra, it is clear that the anomaly changes in certain frequency patterns that are not present in the original audio file due to a decrease in intensity, then from the above results it can also be explained that the insertion of the message in the audio file results in noise in several parts of the frequency spectrum and the most prominent thing in the analysis of this audio file is the occurrence of sound distortion which results in damage to audio quality and has an audio signal pattern that is not sealing related when compared to the original signal pattern, such as the occurrence of repetitive signal patterns or there are truncated parts in the frequency time spectrum. Furthermore, to analyze further related to the numbers contained in the audio file, it is entered into the map application, and the results are directed to a certain place that has been planned by the perpetrator (account A).

CONCLUSIONS

The National Institute of Standards and Technology (NIST) method approach for the analysis of audio files containing hidden text messages in the frequency spectrum has proven that this standard can significantly improve the effectiveness of audio steganography detection. With NIST's ability to detect and analyze abnormal patterns in the frequency spectrum, this research successfully identified hidden messages that were previously difficult to detect with conventional techniques.
The implications of these findings for digital forensic investigations are profound. Firstly, the integration of NIST methods into forensic analysis tools can strengthen steganography detection capabilities in increasingly complex digital environments, particularly in messaging applications such as WhatsApp that use compression and encryption. Secondly, the findings also pave the way for further development of more sensitive and specific steganography detection methods, which can handle a variety of file formats and increasingly sophisticated steganographic techniques.
In the future, strengthening and improving these detection methods will be crucial in ensuring digital security, both for personal data protection and in the context of law enforcement. Improvements to audio steganography detection methods such as the application of transform techniques like Fast Fourier Transformation (FFT), Wavelet Transform, or Short-Time Fourier Transform (STFT) to analyze spectral changes in audio files that may indicate the presence of steganography will not only help in identifying hidden security threats, but will also contribute to

the development of new standards in digital forensics that are more adaptive and responsive to future messaging technologies.

REFERENCES

[1] H. Fayyad-Kazan, S. Kassem-Moussa, H. J. Hejase, and A. J. Hejase, "Forensic Analysis of WhatsApp SQLite Databases on the Unrooted Android Phones," *HighTech Innov. J.*, vol. 3, no. 2, pp. 175–195, 2022, doi: 10.28991/hij-2022-03-02-06.
[2] Ubaidillah *et al.*, "Analysis whatsapp forensic and visualization in android smartphone with support vector machine (SVM) Method," *J. Phys. Conf. Ser.*, vol. 1196, no. 1, 2019, doi: 10.1088/1742-6596/1196/1/012064.
[3] I. Riadi *et al.*, "Forensics Mobile Layanan WhatsApp pada Smartwatch Menggunakan Metode National Institute of Justice," *Jointecs*, vol. 6, no. 28, pp. 63–70, 2021.
[4] H. Shidek, N. Cahyani, and A. A. Wardana, "WhatsApp Chat Visualizer: A Visualization of WhatsApp Messenger's Artifact Using the Timeline Method," *Int. J. Inf. Commun. Technol.*, vol. 6, no. 1, p. 1, 2020, doi: 10.21108/ijoict.2020.61.489.
[5] A. Andria, "Forensik Digital Sistem Informasi Berbasis Web," *JAMI J. Ahli Muda Indones.*, vol. 2, no. 2, pp. 33–44, 2021, doi: 10.46510/jami.v2i2.73.
[6] S. Abd, E. Sarhan, H. A. Youness, and A. M. Bahaa-eldin, "A framework for digital forensics of encrypted real-time network traffic , instant messaging , and VoIP application case study," *Ain Shams Eng. J.*, no. xxxx, p. 102069, 2022, doi: 10.1016/j.asej.2022.102069.
[7] N. Aisyah *et al.*, "Analisa Perkembangan Digital Forensik Dalam Penyidikan Cybercrime Di Indonesia Secara Systematic Review," *J. Esensi Infokom J. Esensi Sist. Inf. dan Sist. Komput.*, vol. 6, no. 1, pp. 22–27, 2022, doi: 10.55886/infokom.v6i1.452.
[8] G. Horsman and N. Sunde, "Unboxing the digital forensic investigation process," *Sci. Justice*, vol. 62, no. 2, pp. 171–180, 2022, doi: 10.1016/j.scijus.2022.01.002.
[9] S. R. Ardiningtias, S. Sunardi, and H. Herman, "Forensik Digital Kasus Penyebaran Pornografi pada Aplikasi Facebook Messenger Berbasis Android Menggunakan Kerangka Kerja National Institute of Justice," *J. Edukasi dan Penelit. Inform.*, vol. 7, no. 3, p. 322, 2021, doi: 10.26418/jp.v7i3.48805.
[10] E. W. Abood *et al.*, "Audio steganography with enhanced LSB method for securing encrypted text with bit cycling," *Bull. Electr. Eng. Informatics*, vol. 11, no. 1, pp. 185–194, 2022, doi: 10.11591/eei.v11i1.3279.
[11] A. A. Permana, "Implementasi Steganography Pada Audio Menggunakan Algoritma End Of File (EOF)," *J. Format*, vol. 9, no. 1, pp. 91–98, 2020.
[12] I. Firman Ashari, "The Evaluation of Image Messages in MP3 Audio Steganography Using Modified Low-Bit Encoding," *Telematika*, vol. 14, no. 2, pp. 133–145, 2021, doi: 10.35671/telematika.v14i2.1031.
[13] L. Chen, R. Wang, D. Yan, and J. Wang, "Learning to Generate Steganographic Cover for Audio Steganography Using GAN," *IEEE Access*, vol. 9, pp. 88098–88107, 2021, doi: 10.1109/ACCESS.2021.3090445.
[14] K. Ying, R. Wang, Y. Lin, and D. Yan, "Adaptive Audio Steganography Based on Improved Syndrome-Trellis Codes," *IEEE Access*, vol. 9, pp. 11705–11715, 2021, doi: 10.1109/ACCESS.2021.3050004.
[15] S. T. Abdulrazzaq, M. M. Siddeq, and M. A. Rodrigues, "A Novel Steganography Approach for Audio Files," *SN Comput. Sci.*, vol. 1, no. 2, pp. 1–13, 2020, doi: 10.1007/s42979-020-0080-2.
[16] J. Wu, B. Chen, W. Luo, and Y. Fang, "Audio Steganography Based on Iterative Adversarial Attacks against Convolutional Neural Networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, no. XX, pp. 2282–2294, 2020, doi: 10.1109/TIFS.2019.2963764.
[17] A. Kuznetsov, A. Onikiychuk, O. Peshkova, T. Gancarczyk, K. Warwas, and R. Ziubina, "Direct Spread Spectrum Technology for Data Hiding in Audio," *Sensors*, vol. 22, no. 9, 2022, doi:

10.3390/s22093115.
[18] A. A. Alsabhany, A. H. Ali, F. Ridzuan, A. H. Azni, and M. R. Mokhtar, "Digital audio steganography: Systematic review, classification, and analysis of the current state of the art," *Comput. Sci. Rev.*, vol. 38, p. 100316, 2020, doi: 10.1016/j.cosrev.2020.100316.
[19] S. G. M. Siregar, "Implementasi Metode Enhanced Audio Steganogafi (EAS) Untuk Penyembunyian Text Terenkripsi Algoritma Gost," *KLIK Kaji. Ilm. Inform. dan Komput.*, vol. 2, no. 1, pp. 20–27, 2021, [Online]. Available: http://www.djournals.com/klik/article/view/220%0Ahttp://www.djournals.com/klik/article/download/220/158
[20] A. A. Pekerti, A. Sasongko, and A. Indrayanto, "Secure End-to-End Voice Communication: A Comprehensive Review of Steganography, Modem-Based Cryptography, and Chaotic Cryptography Techniques," *IEEE Access*, vol. 12, no. March, pp. 75146–75168, 2024, doi: 10.1109/ACCESS.2024.3405317.
[21] H. A. Nassrullah, W. N. Flayyih, and M. A. Nasrullah, "Enhancement of lsb audio steganography based on carrier and message characteristics," *J. Inf. Hiding Multimed. Signal Process.*, vol. 11, no. 3, pp. 126–137, 2020.
[22] B. Qasem, I. Shahadi, M. S. Kod, and H. R. Farhan, "A Review and Comparison for Audio Steganography Techniques Based on Voice over Internet Protocol," vol. 01, no. 02, 2021, [Online]. Available: https://kjes.uokerbala.edu.iq/
[23] S. Jiang, D. Ye, J. Huang, Y. Shang, and Z. Zheng, "SmartSteganogaphy: Light-weight generative audio steganography model for smart embedding application," *J. Netw. Comput. Appl.*, vol. 165, no. March, 2020, doi: 10.1016/j.jnca.2020.102689.

AUTHORS BIBLIOGRAPHY

ABDUL HARIS MUHAMMAD was born in Labuha, South Halmahera on November 17, 1990, current activities as a Lecturer at the S1 Informatics Engineering Study Program - University of Muhammadiyah North Maluku since 2017 and is active in the field of digital forensic research.

GAMARIA MANDAR was born in Ternate on November 20, 1990, Lecturer at the Undergraduate Study Program in Informatics Engineering, University of Muhammadiyah North Maluku since 2019 and is active in the field of Natural languange processing research.